(12) UK Patent Application (19) GB (11) 2 360 610 (13) A

(43) Date of A Publication 26.09.2001

(21) Application No 0007017.7

(22) Date of Filing 22.03.2000

(71) Applicant(s)
Newmark Technology Group Plc
(Incorporated in the United Kingdom)
21/23 Ormside Way, REDHILL, Surrey, RH1 2NT,
United Kingdom

(72) Inventor(s)
Michael Cowen

(74) Agent and/or Address for Service
Beresford & Co
2-5 Warwick Court, High Holborn, LONDON,
WC1R 5DH, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition S)
G4A AAP

(56) Documents Cited
EP 0777171 A1 WO 99/24894 A1 WO 99/11022 A1
WO 98/07249 A1 DE 019843372 A1 US 5821854 A
US 5712973 A

(58) Field of Search
UK CL (Edition R) G4A AAP
INT CL[7] G06F 1/00
ONLINE: EPODOC, WPI, JAPIO

(54) Abstract Title
Computer access control and security system

(57) A computer is provided with an access control device 200, comprising a receiver 205a for receiving a transmission from outside the computer. Access to the computer is inhibited unless the control device receives such a transmission. The transmissions may be periodic and the receiver may be an RF signal receiver. The access control device may be implemented as a PCMCIA card. There is also disclosed a control system for monitoring movement of items of equipment comprising a database storing access data for people associated with such items and means for receiving information identifying the presence of equipment and personnel in a predetermined area. A processor determines, from the database, whether an identified person is authorised to be with that item of equipment. A security device is further disclosed comprising a first transmission means to communicate the status of the security device, an item of equipment or an associated person. A second transmission means has a shorter range than the first so that its transmission can only be detected in the vicinity of a defined area.

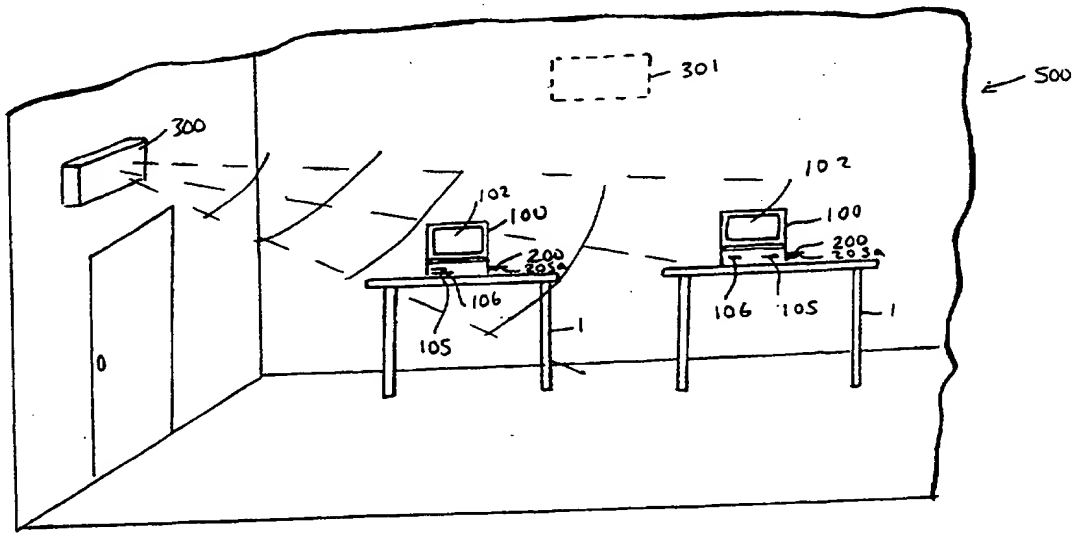

FIG. 1

GB 2 360 610 A

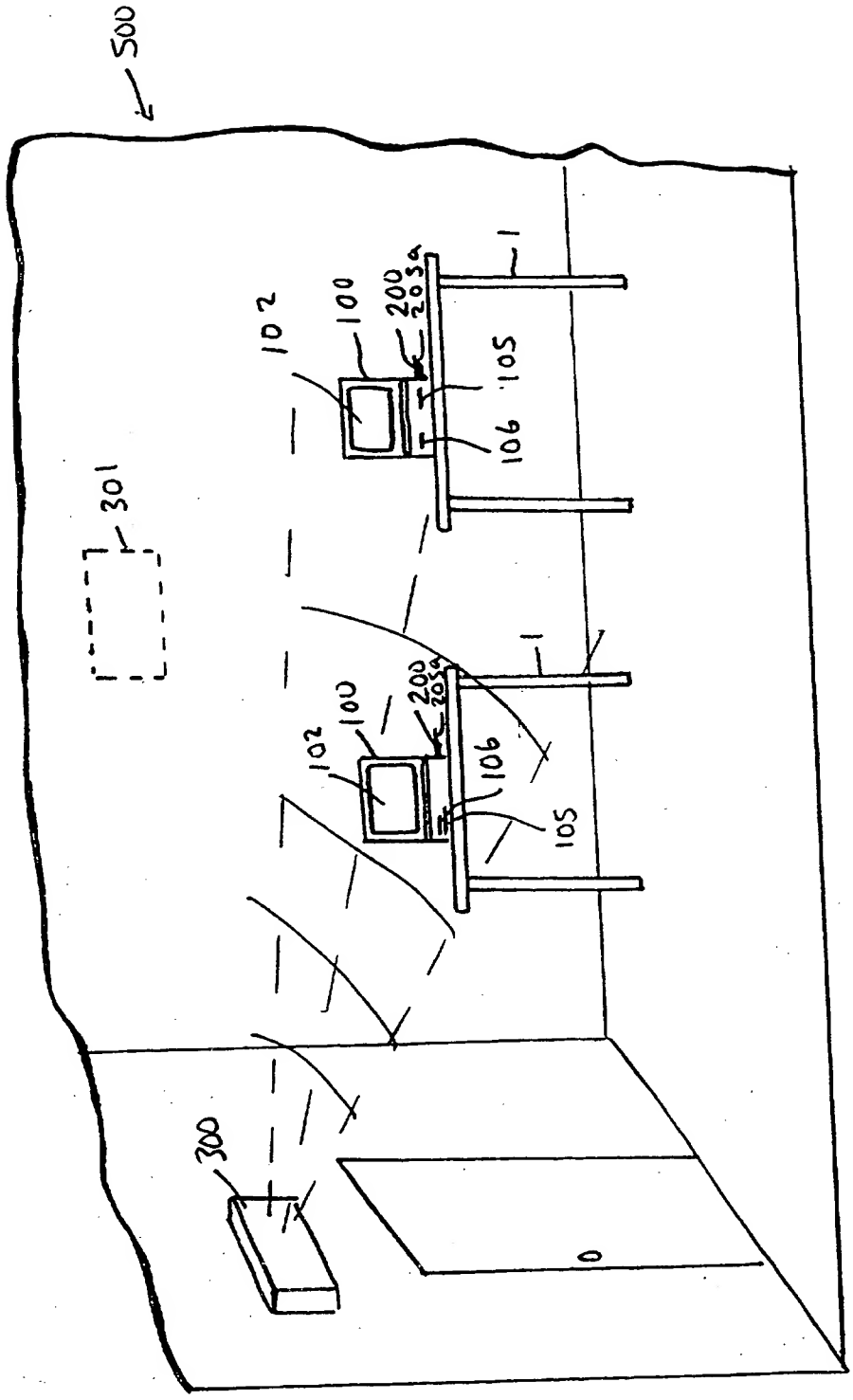

FIG. 1

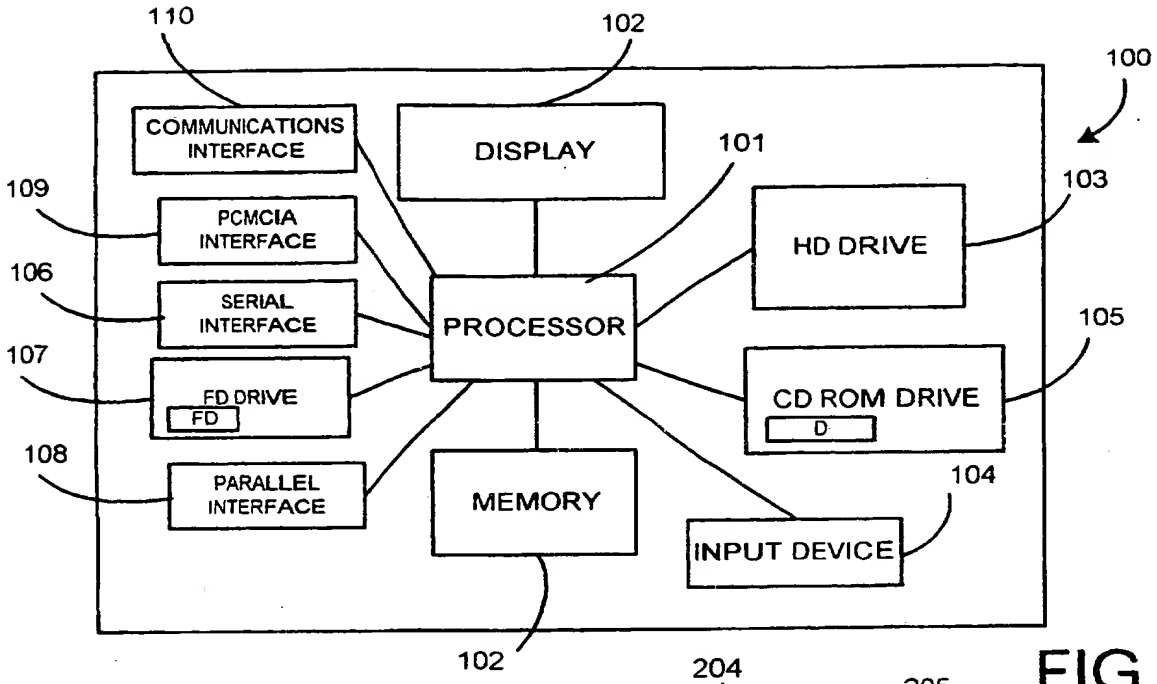

FIG. 2

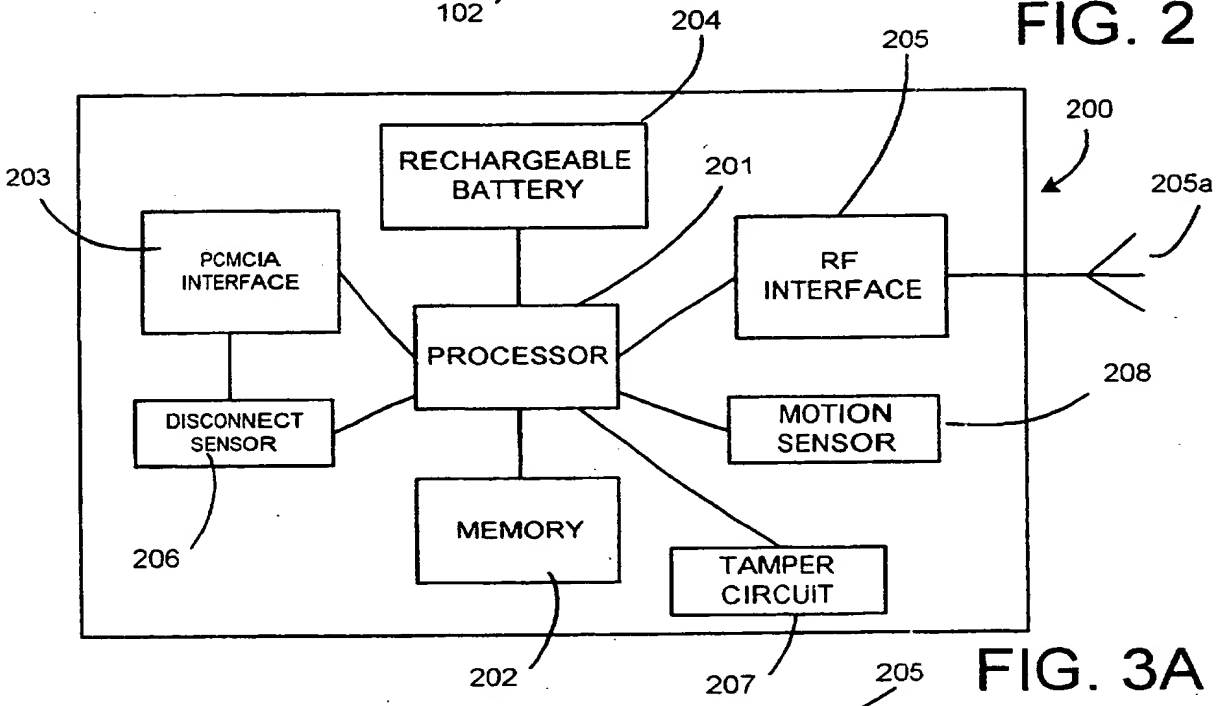

FIG. 3A

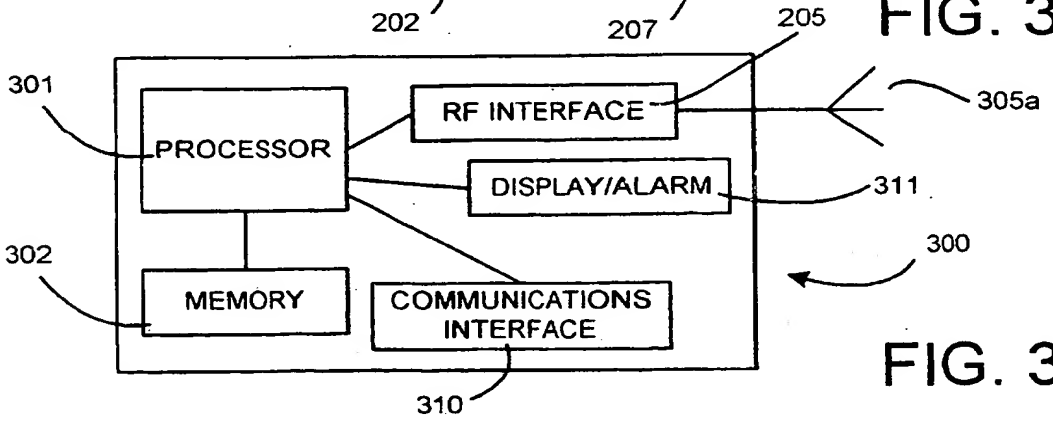

FIG. 3B

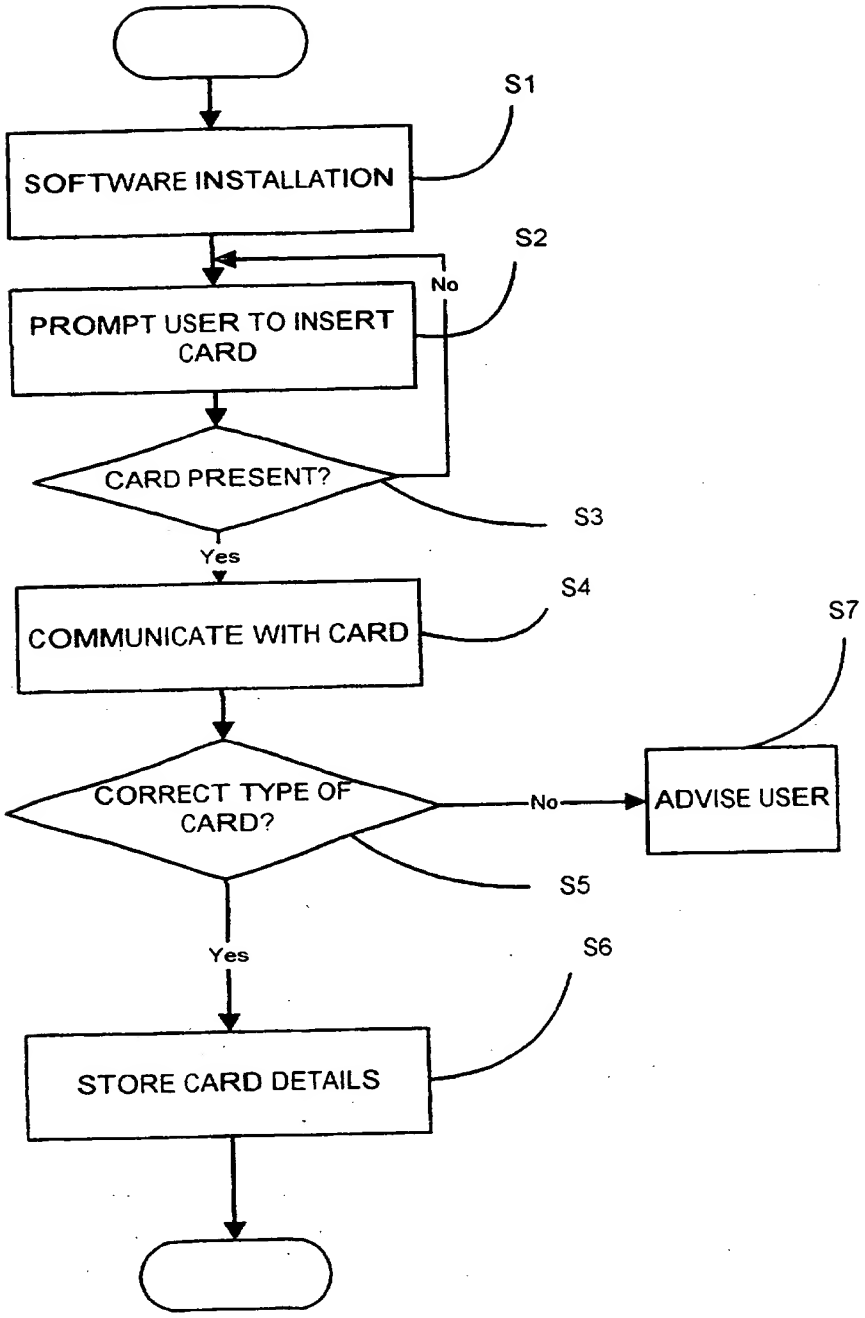
S1
SOFTWARE INSTALLATION
S2
No
PROMPT USER TO INSERT CARD
CARD PRESENT?
S3
Yes
S4
COMMUNICATE WITH CARD
S7
CORRECT TYPE OF CARD?
No
ADVISE USER
S5
Yes
S6
STORE CARD DETAILS

FIG. 4

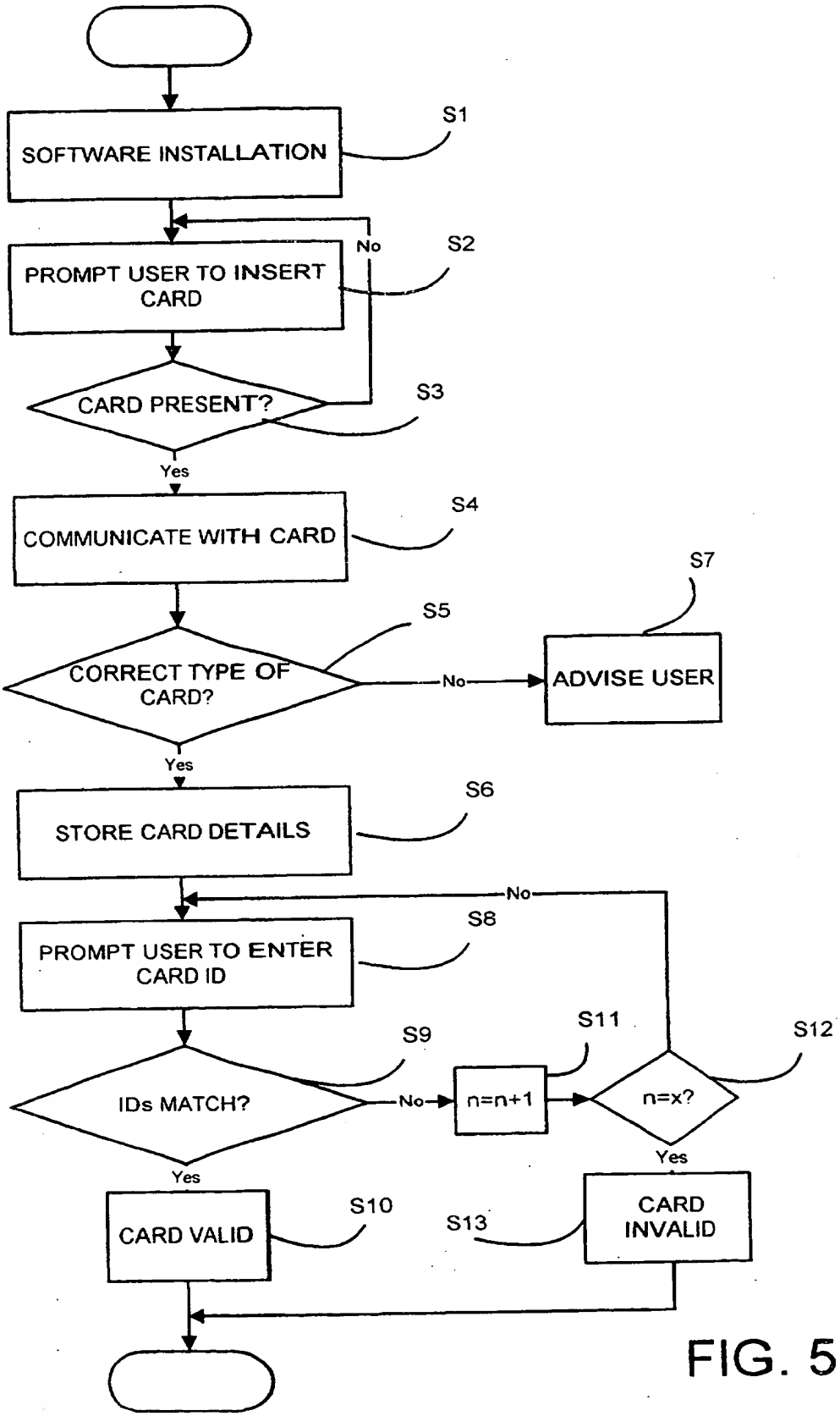
SOFTWARE INSTALLATION
S1
PROMPT USER TO INSERT CARD
No
S2
CARD PRESENT?
S3
Yes
COMMUNICATE WITH CARD
S4
CORRECT TYPE OF CARD?
S5
No
ADVISE USER
S7
Yes
STORE CARD DETAILS
S6
No
PROMPT USER TO ENTER CARD ID
S8
IDs MATCH?
S9
No
n=n+1
S11
n=x?
S12
Yes
Yes
CARD VALID
S10
S13
CARD INVALID

FIG. 5

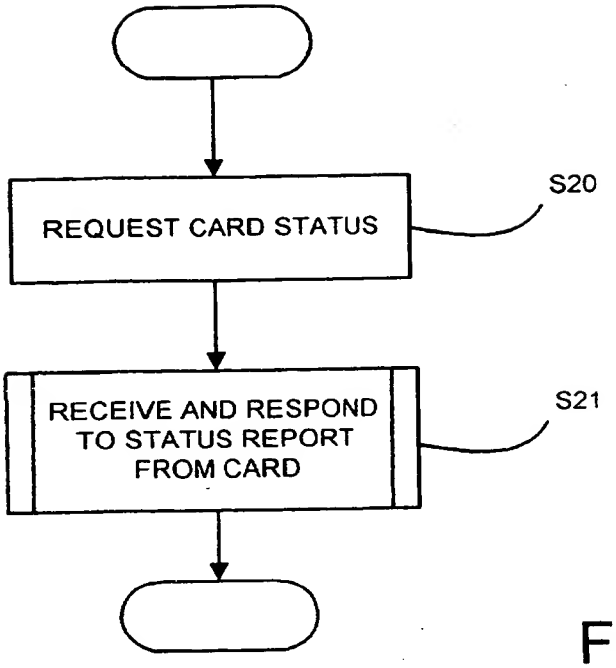
REQUEST CARD STATUS
S20
RECEIVE AND RESPOND TO STATUS REPORT FROM CARD
S21

FIG. 6

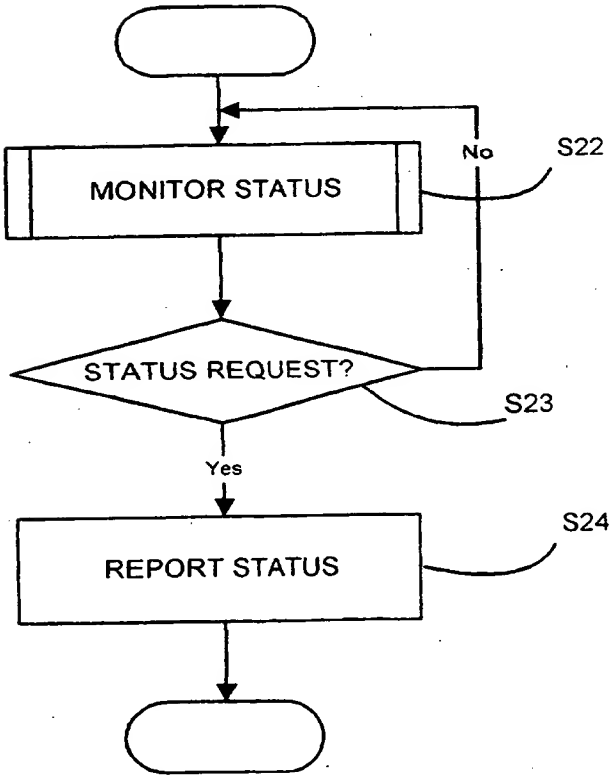
MONITOR STATUS
No
S22
STATUS REQUEST?
S23
Yes
REPORT STATUS
S24

FIG. 7

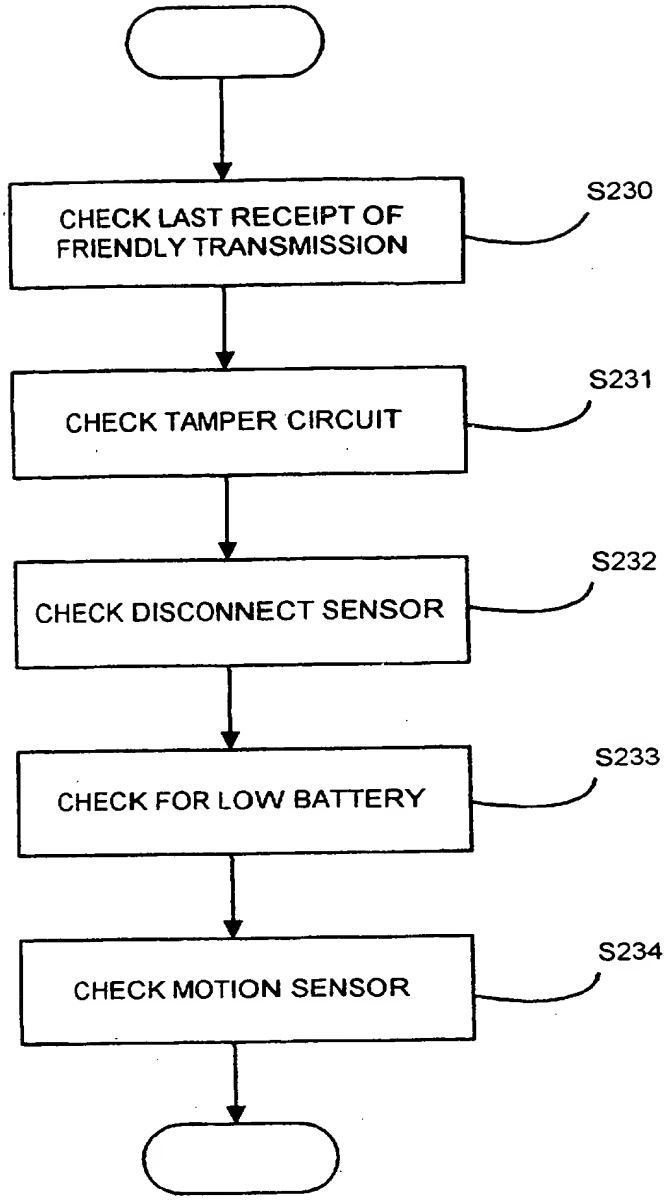
CHECK LAST RECEIPT OF FRIENDLY TRANSMISSION
S230
CHECK TAMPER CIRCUIT
S231
CHECK DISCONNECT SENSOR
S232
CHECK FOR LOW BATTERY
S233
CHECK MOTION SENSOR
S234

FIG.8

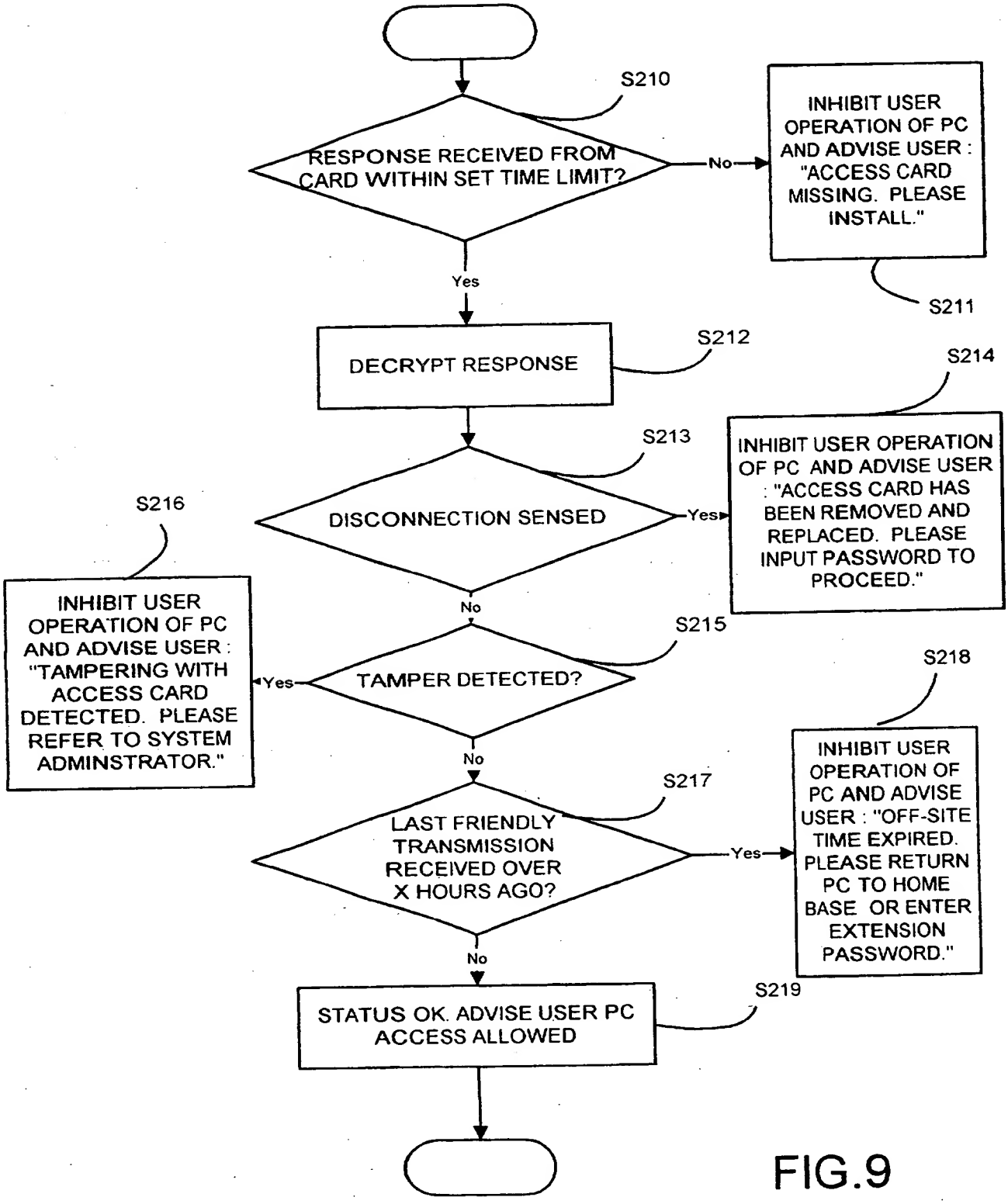
S210
RESPONSE RECEIVED FROM CARD WITHIN SET TIME LIMIT?
No
INHIBIT USER OPERATION OF PC AND ADVISE USER : "ACCESS CARD MISSING. PLEASE INSTALL."
S211
Yes
DECRYPT RESPONSE
S212
S214
S213
DISCONNECTION SENSED
Yes
INHIBIT USER OPERATION OF PC AND ADVISE USER : "ACCESS CARD HAS BEEN REMOVED AND REPLACED. PLEASE INPUT PASSWORD TO PROCEED."
S216
No
S215
INHIBIT USER OPERATION OF PC AND ADVISE USER : "TAMPERING WITH ACCESS CARD DETECTED. PLEASE REFER TO SYSTEM ADMINSTRATOR."
Yes
TAMPER DETECTED?
S218
No
S217
LAST FRIENDLY TRANSMISSION RECEIVED OVER X HOURS AGO?
Yes
INHIBIT USER OPERATION OF PC AND ADVISE USER : "OFF-SITE TIME EXPIRED. PLEASE RETURN PC TO HOME BASE OR ENTER EXTENSION PASSWORD."
No
S219
STATUS OK. ADVISE USER PC ACCESS ALLOWED

FIG.9

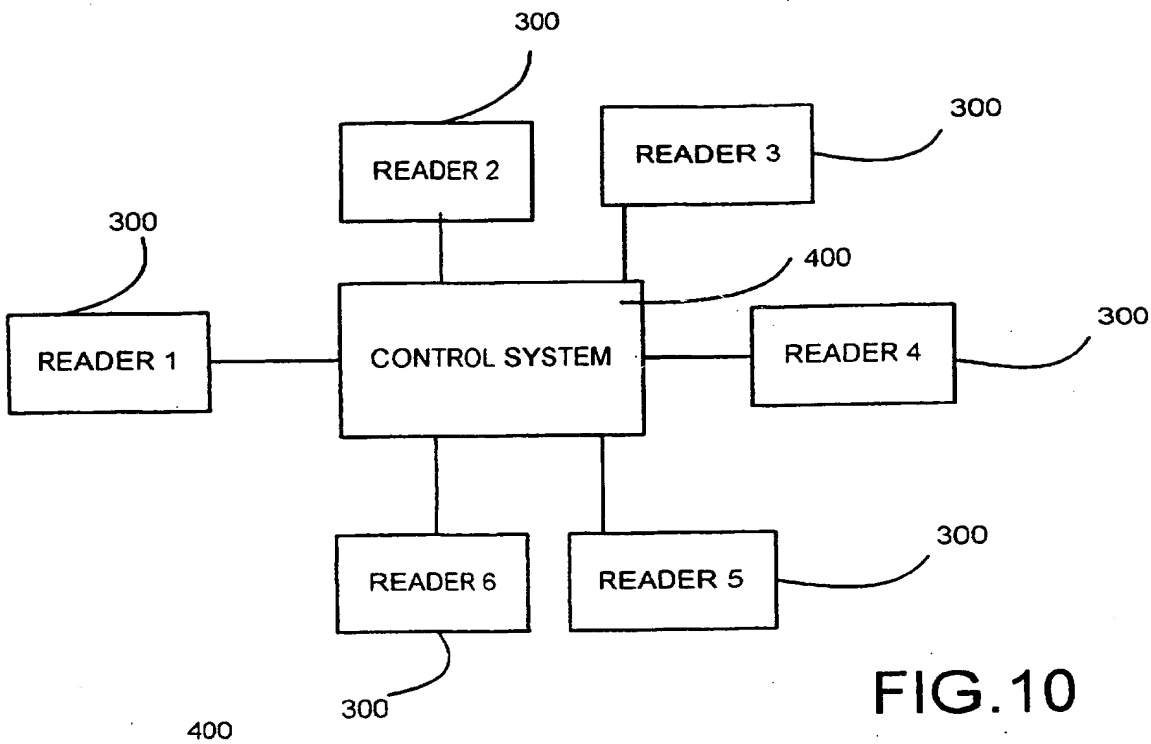
300
READER 2
300
READER 3
300
READER 1
400
CONTROL SYSTEM
READER 4
300
READER 6
READER 5
300
300

FIG.10

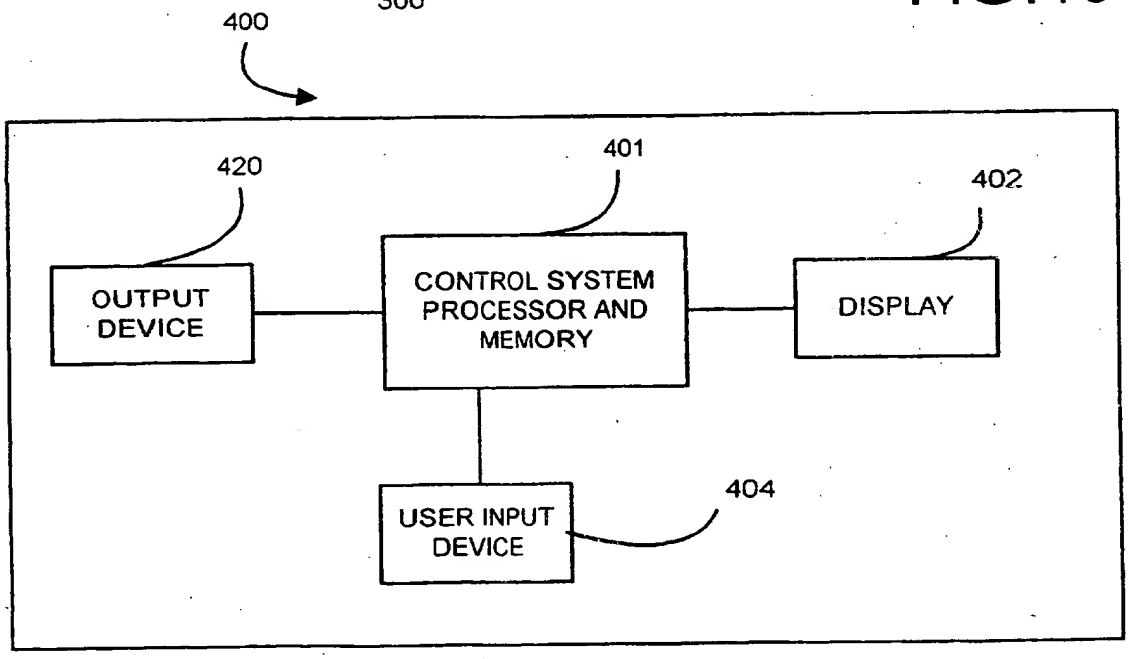
400
420
401
402
OUTPUT DEVICE
CONTROL SYSTEM PROCESSOR AND MEMORY
DISPLAY
404
USER INPUT DEVICE

FIG.11

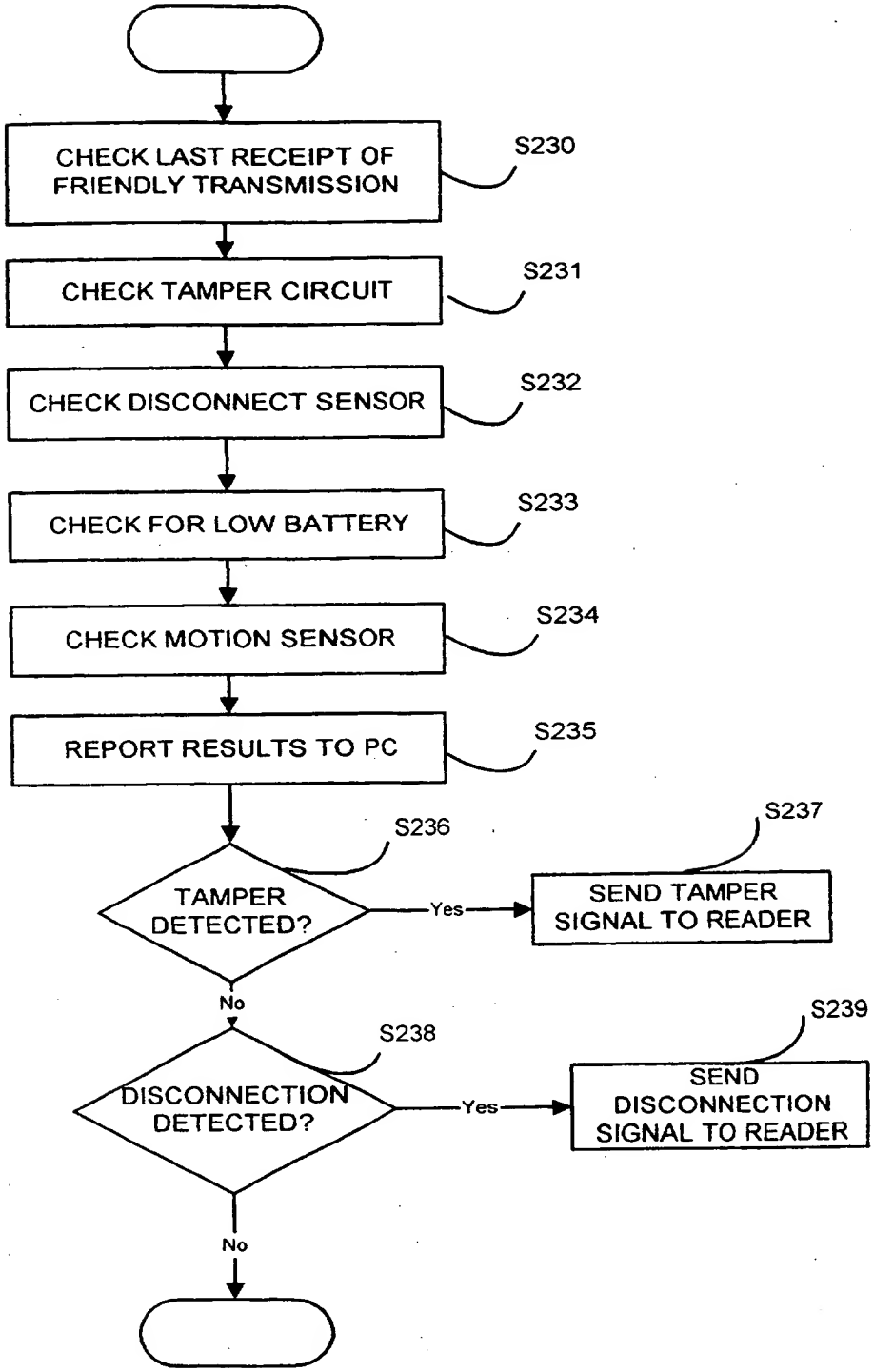
CHECK LAST RECEIPT OF FRIENDLY TRANSMISSION
S230
CHECK TAMPER CIRCUIT
S231
CHECK DISCONNECT SENSOR
S232
CHECK FOR LOW BATTERY
S233
CHECK MOTION SENSOR
S234
REPORT RESULTS TO PC
S235
S236
TAMPER DETECTED?
Yes
S237
SEND TAMPER SIGNAL TO READER
No
S238
DISCONNECTION DETECTED?
Yes
S239
SEND DISCONNECTION SIGNAL TO READER
No

FIG.12

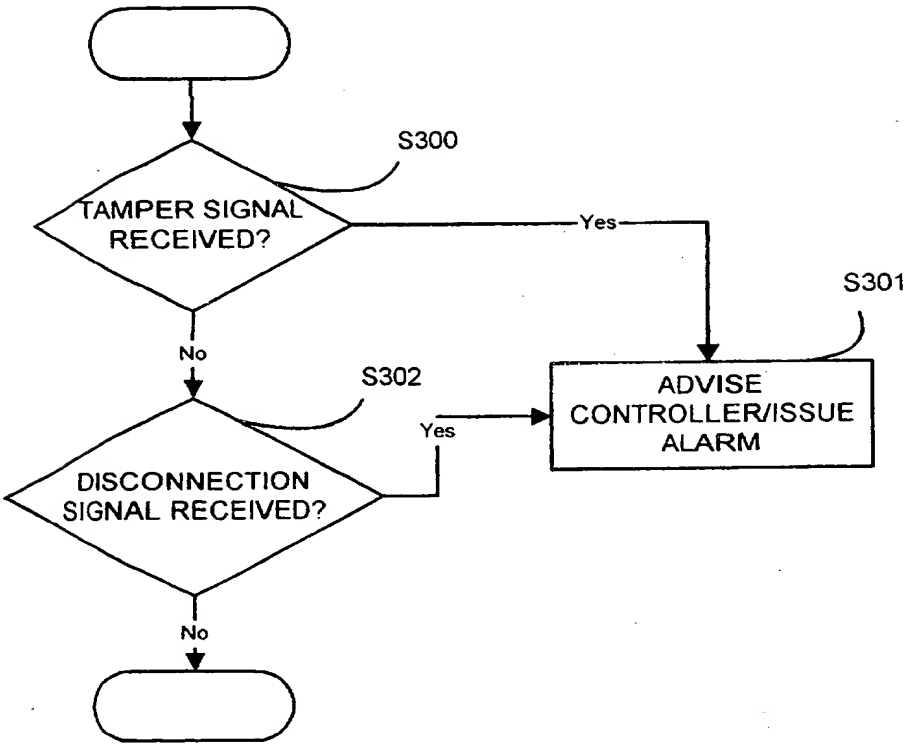
S300
TAMPER SIGNAL RECEIVED?
Yes
S301
No
S302
ADVISE CONTROLLER/ISSUE ALARM
Yes
DISCONNECTION SIGNAL RECEIVED?
No

FIG.13

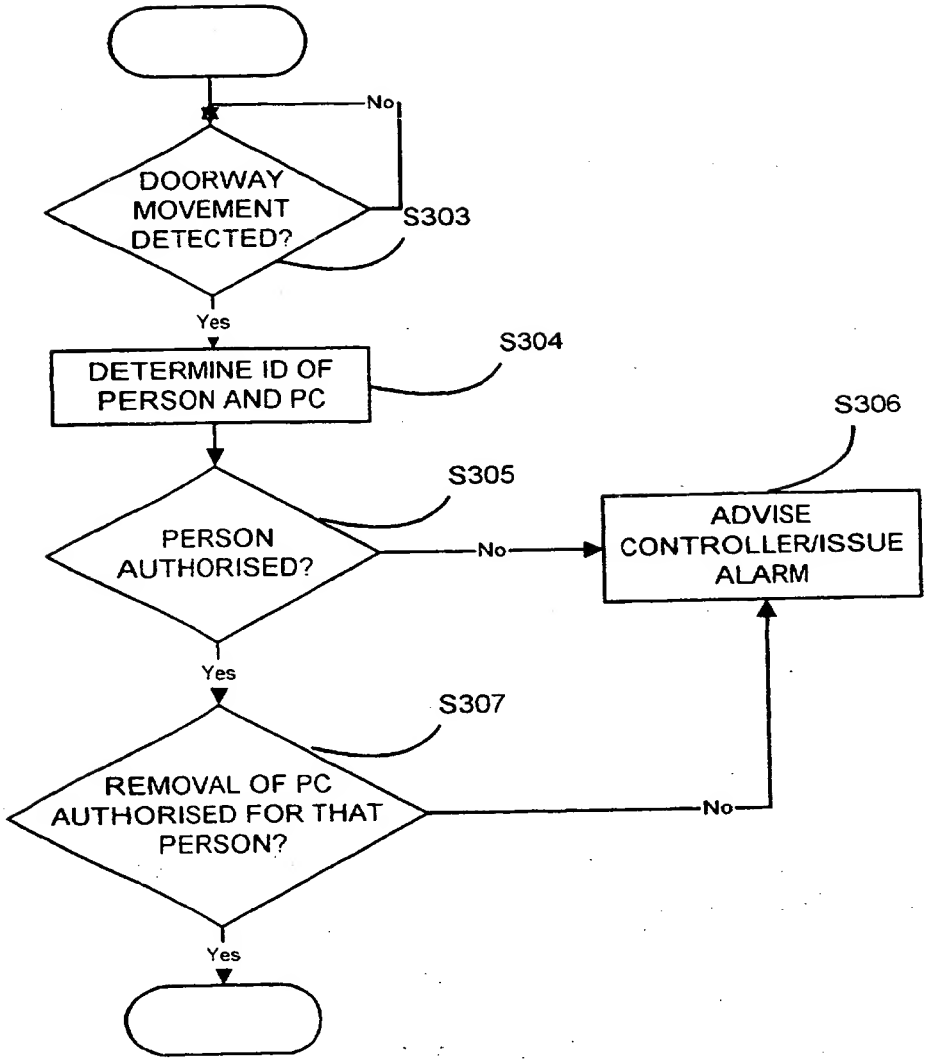
No
DOORWAY MOVEMENT DETECTED?
S303
Yes
DETERMINE ID OF PERSON AND PC
S304
S306
S305
PERSON AUTHORISED?
No
ADVISE CONTROLLER/ISSUE ALARM
Yes
S307
REMOVAL OF PC AUTHORISED FOR THAT PERSON?
No
Yes

FIG.14

AN ACCESS CONTROL SYSTEM

This invention relates to a system and device for controlling access to an item of equipment such as a personal computer or the like and to an item of equipment having an access control device or mechanism.

Security systems such as the PARSEC (trade mark) personnel and article security tagging systems produced by Newmark Technology enable movement of assets such as items of equipment, for example personal computers, particularly portable computers such as laptops, notebooks or palm tops, and the like to be monitored. Such systems enable unauthorised movement or removal of such an asset to be detected and, if desired, intercepted.

It is an aim of the present invention to provide a system and a device for controlling access to a computer or microprocessor controlled item of equipment such as a personal computer, in particular a portable computer, and to provide an item of equipment having a device for controlling access to that device.

In one aspect, the present invention provides a computer

or a computer-controlled item of equipment having processor means operable to prevent or inhibit user operation of the computer if a transmission has not been received from another device within a predetermined time.

In one aspect, the present invention provides a computer or a computer-controlled item of equipment having an access control device comprising means for receiving a predetermined transmission, and means for inhibiting or preventing user operation of the computer when a predetermined time has elapsed since the receipt of a predetermined transmission by the access control device. The transmission may be a RF (Radio Frequency) transmission and the receiving means RF signal receiving means.

In one aspect, the present invention provides a computer or a computer-controlled item of equipment adapted to prevent or inhibit user operation of the computer if an access control means has been tampered with or has been disconnected from the computer.

In one aspect, the present invention provides a computer or a computer-controlled item of equipment having processor means operable to prevent or inhibit completion

of a booting up procedure unless an access control device meeting certain requirements is coupled to or incorporated in the computer. The processor means may be operable to determine that the access control device does not meet the requirements if the access control device does not report receipt of a predetermined transmission from outside the computer within a predetermined time.

In one aspect, the present invention provides a computer or a computer-controlled item of equipment having processor means operable to prevent or inhibit writing to or reading from a memory such as a hard disc unless an access control device meeting certain requirements is coupled to or incorporated in the computer. The processor means may be operable to determine that the access control device does not meet the requirements if the access control device does not report receipt of a predetermined transmission from outside the computer within a predetermined time.

In one aspect, the present invention provides an access control device for a computer or a computer-controlled item of equipment, the access control device comprising means for communicating status information to the computer to enable access to use of the computer by a

user to be inhibited or prevented unless the status of the access control device is determined to be acceptable. The processor means may be operable to determine that the access control device does not meet the requirements if the access control device does not report receipt of a predetermined transmission from outside the computer within a predetermined time.

In one aspect, the present invention provides an access control device for a computer or a computer-controlled item of equipment, the access control device comprising means for receiving a transmission from a device other than the computer and means for communicating information regarding receipt of the transmission to the computer to prevent or inhibit access to use of the computer by a user when a predetermined time has elapsed since the receipt of a transmission by the access control device.

In one aspect, the present invention provides an access control device for a computer or a computer-controlled item of equipment, the access control device comprising means for determining information as to whether the access control means has been disconnected from the computer or has been tampered with and means for communicating information to the computer to prevent or

inhibit access to use of the computer by a user when the access control device has been disconnected or otherwise tampered with. The processor means may be operable to determine that the access control device does not meet the requirements if the access control device does not report receipt of a predetermined transmission from outside the computer within a predetermined time.

The access control device may comprise means for transmitting information to a security control system. The access control device may comprise a PCMCIA (Personal Computer Memory Card International Association) card.

In one aspect, the present invention provides an item of equipment comprising such a computer, device or PCMCIA. In one aspect, the present invention provides a security system comprising a plurality of such items of equipment and means for detecting the presence of an item of equipment in the vicinity of a doorway, exit or other defined area such as, for example, an area to which access by the item of equipment is prohibited, for example a clean room.

Embodiments of the present invention will now be described, by way of example, with reference to the

accompanying drawings, in which:

Figure 1 shows very diagrammatically a perspective view of part of a room such as an office housing a number of portable computers having devices in accordance with the present invention for controlling access to the portable computers;

Figure 2 shows a functional block diagram of one of the portable computers shown in Figure 1;

Figure 3A shows a functional block diagram of a PCMCIA card comprising a device for controlling access to a portable computer;

Figure 3B shows a functional block diagram of a transmission generating device shown in Figure 1;

Figure 4 shows a flow chart for illustrating one example of a method of installing the PCMCIA card shown in Figure 3 and the associated software into a portable computer as shown in Figure 1;

Figure 5 shows a flow chart similar to Figure 4 illustrating another example of a method of installing

the PCMCIA card shown in Figure 3 and the associated software into a portable computer as shown in Figure 1;

Figures 6 and 7 show top level flow charts illustrating one example of functions carried out by the portable computer and the PCMCIA card to enable the portable computer to determine the status of the PCMCIA card;

Figure 8 shows a flow chart illustrating in greater detail steps that may be carried out by the PCMCIA card shown in Figure 3A to check its status;

Figure 9 shows a flow chart illustrating in greater detail steps that may be carried out by a portable computer in response to a status report received from its PCMCIA card;

Figure 10 shows a simplified functional block diagram of one example of a security system that may use an access control arrangement;

Figure 11 shows a functional block diagram of an example of a control system of the security system shown in Figure 10;

Figure 12 shows a flow chart similar to Figure 8 but illustrating one example of further steps that may be carried out by the PCMCIA card when the associated portable computer is included in the security system shown in Figures 10 and 11;

Figure 13 shows a flow chart for illustrating overall operation of the security system shown in Figures 10 and 11; and

Figure 14 shows a flow chart for illustrating the response of the control system shown in Figures 10 and 11 to signals received from a PCMCIA card.

Referring now to the drawings, Figure 1 shows a very diagrammatic perspective view of part of an office 500 within a building. As shown in Figure 1, the office includes one or more (two are shown) desks or tables 1 on each of which is provided at least one portable computer 100. The portable computer may be, for example, a so-called laptop or notebook computer having a LCD or similar screen and being designed to be easily moved between locations by a user.

Figure 2 shows functional components of one of the

portable computers 100 such as a notebook or laptop. As shown, and as is well known in the art, the computer 100 comprises a processor or main unit 101 having associated memory 102 in the form of RAM and/or ROM. The processor 101 is coupled to a display device 102, generally an LCD display device, a hard disk drive 103, an input device 104 which generally consists of, in the case of a laptop or notebook computer, a keyboard and a touch pad or other integral pointing device. Generally, the computer 100 will also have a removable disk disk drive. In the example shown, the computer 100 has a CD or DVD ROM drive 105 for receiving a CD or DVD disc D and a floppy disk drive 106 for receiving a floppy disc F. The computer 100 also has a number of interfaces for enabling connection to external devices or cards. In the example shown, the computer 100 has one serial interface port 107 for enabling connection of, for example, a mouse or other serial device and a parallel interface port 108 which would generally be used for connection to a printer. The computer 100 also has a PCMCIA (Personal Computer Memory Card International Association) interface port 109 for receiving a PCMCIA card 200 (Figure 1) which, in this embodiment, provides the device for controlling access to operational functions of the computer. As is known in the art the computer 100 may

have one or more additional PCMCIA ports for receiving a MODEM or the like.

Figure 3A shows a block schematic diagram of functional components of the PCMCIA card 200.

As shown in Figure 3A, the PCMCIA card 200 comprises a processor 201 having associated memory 202, generally in the form of ROM, carrying processor implementable instructions and possibly also data for causing the PCMCIA card 200 to carry out the functions that will be described below. The processor 201 is coupled to a PCMCIA interface 203 which enables interfacing between the functional components of the PCMCIA card 200 and the computer 100 when the card is inserted into the PCMCIA interface port 109 of the computer. The card 200 also carries a rechargeable battery 204 which, when the card is inserted into the computer 100, is recharged from the power supply (not shown in Figure 2) of the computer 100. Generally, the power supply of the computer 100 will consist of an internal rechargeable battery but, as is well known in the art, the computer 100 will also have the facility for operating from the mains AC supply via a transformer. Although not shown in Figure 3A, the rechargeable battery 204 provides the power supply for

all the functional components of the PCMCIA card 200. Normally, the card 200 will draw on the computer's power supply and will only draw on the rechargeable battery 204 when the computer 100 is switched off. The PCMCIA card 200 also has an RF (radio frequency) interface having an RF transponder including an RF antenna 205a for enabling, as will be described in detail below, receipt of RF signals from an RF signal transmission device 300 (see Figure 1). The card 200 also includes a disconnect sensor 206 for detecting when the card 200 has been electrically or physically disconnected from the computer 100 by removal from the PCMCIA port 109. For example, the disconnect sensor 206 may be arranged to determine whether any one of the multiple common ground pins of the PCMCIA interface 203 has been disconnected from the others. The card shown in Figure 3A also has a tamper circuit 207 which detects any tampering with the physical and/or electrical integrity of the card and a motion sensor 208 for detecting movement of the card. The tamper circuit 207 may include an electrical path (for example a frangible seal) which is broken when the casing of the PCMCIA card is opened and a device for detecting when that electrical path is broken. The motion sensor may, for example, consist of one or more tilt switches or acceleration sensing devices received within an opening

of the PCB of the PCMCIA card.

Figure 3B shows functional components of the RF signal transmission device 300 which, as will be described in detail below, is arranged to generate an RF signal having a range such that the transmission should be received by the antennas 205a of PCMCIA cards 200 located within the room shown in Figure 1. As shown in Figure 3B, the RF signal transmission device 300 comprises, in this example, a processor 301 and associated memory 302, an RF interface 305 having an RF transponder and an RF antenna 305a and optionally a communications interface 310 for enabling communication with, for example, a central control station. This communications interface 310 and the RF interfaces described above may be similar to those used in the applicant's existing PARSEC personnel and article security tagging system with the PCMCIA card being arranged to receive RF signals from the RF signal transmission device 300.

The PCMCIA cards 200 are manufactured using known PCMCIA techniques and are dimensioned so as to fit in the PCMCIA interface ports 109 of the portable computers such that the part of the card carrying the antenna 205a projects from the PCMCIA port 109 as shown schematically in

Figure 1 to facilitate reception of RF signals from the RF signal transmission device 300 by the RF interface 205.

Figure 4 shows a flow chart for illustrating how a portable computer 100 is modified to provide controlled access to its operation.

At step S1 in Figure 4 software is installed onto the hard drive 103 or other permanent internal memory of the portable computer 100. The software may be supplied on a floppy disk F (Figure 2) insertable into the floppy disk drive 106 or more commonly on a CDROM or DVD disc D insertable into the CD or DVD ROM drive 105 (Figure 2). As another possibility, where the portable computer 100 has a communications interface 110 (Figure 2) such as a MODEM, infrared link or network connection, then the software may be supplied as a signal using that communications interface. If the portable computer is a palm top rather than a personal computer the permanent internal memory will generally be a flash RAM onto which the software may be pre-stored in known manner.

The software installed at step S1 modifies the operational system of the computer 100. The software may

form an extension of the operating system BIOS (Basic Input/Output System) which modifies the checks carried out by the computer when the computer is initially switched on or booted up so that, in addition to the conventional checks, a further check is added which requires the presence of the correct PCMCIA card 200 in the PCMCIA port 109 before the computer will boot up. This may be achieved by a modification of the BIOS password validation software that is found on some laptops or notebooks so that instead of looking for a password the BIOS causes the processor to check for the presence of a valid PCMCIA card 200. Alternatively, where the computer uses a Microsoft (trade mark) Windows (trade mark) or similar operating system, then the software may consist of an extension of the Windows operating system which causes the operating system to check for the presence of the correct PCMCIA card 200 in the PCMCIA port 109 before data can be read from or written to the hard disk drive 103 so that, for example, the PCMCIA card forms part of the encryption/decryption used in all disk read and write operations.

Once the software has been installed as discussed above, the software causes the processor 101 of the computer 100 to display on the display 102 a message to the user at

step S2 prompting the user to insert the PCMCIA card 200 into the port 109. At step S3, the processor 101 checks to see whether the card 200 has been inserted and, until the answer at step S3 is "yes", the prompt to the user to insert the card remains displayed on the display 102.

When the answer at step S3 is "yes", the processor 101 commences communication with the card 200 at step S4. This communication is encrypted using an encryption algorithm installed in the software installation step S1. In this example, the processor 101 sends the card an encrypted message requesting the processor 201 of the card to supply, using the encryption algorithm, its identity code to the processor 101.

If the processor 101 receives from the card 200 information which, when decrypted in accordance with the encryption algorithm installed at step S1, the processor 101 recognises as a card identification number, then the processor 101 determines at step S5 that the correct type of card has been installed in the PCMCIA port 109 and stores the card details, in particular the identity number of the card, in its memory 102 at step S6.

If the card 200 does not respond to the processor 101 at

step S4 or the return communication from the card cannot be decrypted by the processor 101 to provide information identifiable as a card identification number, then the processor 101 determines at step S5 that the card is incorrect and advises the user accordingly at step S7. For example, the processor 101 may cause the user to be displayed a message such as "incorrect card inserted please contact the system controller". Such a message may be displayed when, for example, a user inadvertently inserts a conventional PCMCIA card such as a modem or similar device or when the user inserts a card 200 which operates using a different encryption algorithm. The user may then contact the system controller to obtain a correct card.

Figure 5 shows a flow chart similar to Figure 4 in which, after step S6 has been carried out, the processor 101 causes, at step S8, the display 102 to display a message prompting the user to enter a card ID provided to him by the system controller with the card. The processor 101 then checks at step S9 whether the ID read from the card 200 itself by the processor 101 matches that input by the user. If the answer is "yes", then the processor 101 confirms that the card is valid at step S10. If, however, the answer at step S9 is "no" then the processor

101 increments a counter by one at step S11, checks at step S12 whether the count equals x and, if not, prompts the user again to enter the card number. Steps S8 to S12 are repeated until n = x so that the user has x opportunities to enter the correct ID. For example x may be three. The time allowed for entry of the correct password may also be limited.

If the user has not entered the correct ID by, in this example, the third attempt, then the processor 101 determines at step S13 that the card ID is invalid and advises the user accordingly. The extra steps shown in Figure 5 provide additional security so that, even if a valid card is acquired by an unauthorised user, that card cannot be rendered effective because the unauthorised user will not have access to the separately supplied card ID code.

Figure 6 shows a top level flow chart for illustrating the steps carried out by the processor 101 of the personal computer in order to control access to use of the personal computer. As indicated above, the steps may be carried out during boot-up of the computer or prior to writing to or reading data from the hard disk drive 103. Thus, at step S20 the processor 101 sends an encrypted

communication to the card 200 via the PCMCIA interface requesting the card 200 to advise its current status and then, as will be described in greater detail with reference to Figure 9, at step S21 receives and responds to any encrypted communication received from the card 200 in response to its request.

As shown in Figure 7, the card 200 continuously monitors its status at step S22 as a background task. When a request for status information is received from the processor 101 at step S22, the card 200 reports its status to the portable computer at step S24 as will be described in greater detail below.

As shown schematically in Figure 1, the RF signal transmission device 300 periodically sends out an RF signal having a range sufficient for the signal to be received by the antennae 205a of any PCMCIA cards 200 within the room. Each time a PCMCIA card 200 receives such a signal from the RF signal transmission it restarts an internal counter of the processor arranged to count the time since receipt of the last transmission from the RF signal transmission device 300. The RF signal transmissions from the RF signal transmission device 300 may be, for example, hourly and may be programmable to

meet customer requirements. The RF signal thus acts as a "home" or "friendly" signal to advise the card (and thus the portable computer) that it is still in its intended location, for example, the office shown in Figure 1.

Figure 8 shows in greater detail the status checks carried out by the processor 201 at step S22 in Figure 7. Thus, at step S230, the processor 201 accesses its memory 202 to check the count of the counter determining the time since the last receipt of a transmission from the RF signal transmission device 300. The processor 201 may also carry out further status checks. Thus, in this example, the processor 201 also checks at step S231 the status of the tamper circuit 207 to determine whether any attempt has been made to open the cover of the card 200 itself. The processor 201 also checks at step S232 in Figure 8 whether the disconnect sensor 206 has detected any disconnection of the card from the PCMCIA interface port 109, that is whether the card 200 has been removed and replaced. The processor 201 may also check at step S233 whether it is receiving a low battery signal from the rechargeable battery 204 and, if a motion sensor 208 is provided on the card 200, checks whether the motion sensor 208 has detected any movement at step S234. Steps

S230 to S234 may be carried out in any order as determined by the processor 201 of the card.

The card processor 201 sends an encrypted communication over the PCMCIA interface to the processor 101 of the portable computer reporting the results of these checks at step S24 in Figure 7.

The card processor 201 may simply report to the portable computer whether or not its status is satisfactory, that is whether or not all of the status checks were passed. As one possibility, the card may simply not respond if the status checks were not passed. In the event that the computer processor 101 does not receive a "status OK" signal (because the status of the card is not satisfactory or the card is missing) within a predetermined time from its request for status information, then the processor 101 will inhibit user operation of the portable computer. As indicated above, where the validity or status of the card is checked during boot-up, then user operation of the computer 100 may be inhibited by the processor 101 refusing to complete the boot-up procedure if the card's presence is not detected. If the presence or validity of the card is checked after boot-up of the computer, then the processor

101 may inhibit user operation of the personal computer by not carrying out any instructions to read or write to the hard disk drive.

The card processor 201 may, however, provide a detailed report of the status check results to the portable computer. Figure 9 shows in greater detail the operations that may be carried out by the processor 101 at step S21 of Figure 6 when the card provides a detailed status report. At step S210, the processor 101 waits for a response from the card 200 to the request issued at step S20 in Figure 6. If no response is received from the card within a predetermined set time limit, then the processor 101 assumes that the card is missing from the PCMCIA port 109 and inhibits user operation of the portable computer 100 as described above at step S211. At this step S211 the processor 101 also causes the display 102 to display a message to the user indicating that the card 200 is missing and must be installed in order to enable user operation of the computer.

If, however, a response is received from the card at step S210, the processor 101 decrypts the response at step S212 using the decryption algorithm included in the software installed at step S1 and then checks the

decrypted status information. Thus, at step S213, the processor 101 checks whether the decrypted status information indicates that disconnection of the card 200 has been sensed. If the answer is "yes", then at step S214, the processor 101 inhibits user operation of the PC as set out at step S211 and advises the user that the access card has been removed and replaced and that a password (or a signal from the system administrator where, for example, the portable computer is connected to a network) is required to enable user operation of the portable computer 100. For example, the processor 101 may cause the display 102 to display to the user the message "access card has been removed and replaced. Please input password to proceed." If, in response, the user inputs the correct password then the processor 101 allows the user access to the portable computer 100. Otherwise the processor 101 continues to inhibit user operation of the computer 100.

If the answer at step S213 is no, then the processor 101 checks whether the status information indicates any tampering with integrity of the card at step S215. If tampering is indicated, then the processor 101 inhibits user operation of the portable computer 100 at step S216 and advises the user that the card has been tampered

with. For example, the processor 101 may cause the display to display the message: "Tampering with access card detected. Please refer to system administrator.". In this embodiment, therefore, any detected tampering will result in a referral to the system administrator who may issue a new card for that portable computer 100 and also conduct investigations into the tampering.

If the answer at step S215 is "no", then the processor 101 checks whether the received status information indicates that the last transmission from the RF signal transmission device 300 was received greater than a predetermined time (X hours) ago at step S217. In this embodiment, the software installed at step S1 on the portable computer 100 gives the allowable value of the time period "X hours" and this time period may vary from portable computer to portable computer allowing, for example, certain portable computers to be removed from the vicinity of the transmission device 300 to enable, for example, the user to operate in a different part of the building or to take the portable computer home for work purposes. The time period set for a given portable computer may be adjustable by a system controller who has password access to the appropriate part of the software. If the answer at step S217 is "yes", then the processor

101 inhibits user operation of the portable computer 100 as described above with reference to step S211 and advises the user that the portable computer 100 must either be returned to its home base or a password entered to extend the off-site time by, for example, displaying the message "Off site time expired. Please return portable computer to home base or enter extension password.". When the portable computer is returned to its home base after expiry of the off-site time (whether or not extended by use of the password) then reinstallation of the card or action by the system administrator may be required. As another possibility inhibition of user operation of the portable computer may be automatically removed without any need for further action by the user (such as, for example, reinstallation of the card or inputting of a password) when the card next detects a transmission from the RF signal transmission device 300.

If the answer at step S217 is "no", then, in this embodiment, the portable computer 100 allows the user access to the computer by, as detailed above, either completing the boot-up procedure or enabling reading and writing to the hard disk drive.

As shown in Figure 3a, the card 200 may also include a motion sensor 208 and, as set out in Figure 8, the processor 201 may check the motion sensor status at step S234 in addition to the other checks. However, where, as in the example described above, the access-controlled device is a stand-alone device, that is where neither the card nor the portable computer reports information regarding its status to another device, then the output of the motion sensor will not be used and the card processor 201 will be programmed so as to ignore the motion sensor output and will report a satisfactory status regardless of the motion sensor output. Where the card 200 is intended only for use as a stand-alone device then the motion sensor may be omitted. Indeed, where the access-controlled device is a stand-alone device then the card 200 may only be provided with the RF signal transmission detection arrangement so that user operation of the portable computer is only inhibited if the card is missing or the portable computer has not received a signal from the RF signal transmission device 300 within the required time limit. The presence of the disconnection and/or tamper circuits is however advantageous in that they should enable detection of any attempt to circumvent the access control.

Where, as set out in Figure 8, the card 200 also checks to determine whether its battery voltage is within acceptable limits, then, when the processor 101 detects in the decrypted response that the card battery voltage is low, the processor 101 may, while still allowing the user access to use of the personal computer 100, issue a warning to the user (for example by displaying a message on the display 102) that the card's battery voltage is getting low and that the portable computer should be connected, via a transformer, to the mains supply to enable recharging of its own and the card's rechargeable battery.

In the embodiment described above, it is the programming of the processor 101 that determines the period of time (x hours) allowed between receipt of friendly transmissions. It will, however, be appreciated that the period allowed between receipt of "friendly" or "home" transmissions from the RF signal transmission device may be stored in the memory 202 of the card 200 so that the card processor 201 determines whether a "friendly" or "home" transmission has been received in time and simply reports to the processor 101 whether or not the transmission was received in time. This would enable, for example, the off-site time allowed for a particular

portable computer to be changed relatively easily by changing the card 200 for a different card allowing for a different length of off-site times.

The embodiment described above is a stand-alone system in which reports regarding the status of a card 200 are supplied only to the portable computer 100 carrying that card.

In the above-described embodiments, the cards 200 need only be capable of receiving RF signals. Generally, however, the RF transponders of the cards may also be capable of sending RF signals under control of the processor 201 so that each card 200 can report its status not only to the processor 101 of the computer within which the card is installed but also to a reader which may, as shown in Figure 1, be provided as part of the RF signal transmission device 300. This reader 300 may itself be a stand-alone device incorporating an alarm (311 in Figure 3B) capable of issuing an alarm when it receives an RF signal from a card 200 indicating that the status of the card is not acceptable, for example indicating that the card has been disconnected and reinserted or tampered with.

The reader 300 may also incorporate the functional features of a reader of Newmark Technology's existing PARSEC system so as to enable the reader to determine when a portable computer is in the vicinity ("vicinity detection") of an exit or door 400 of the office in the example shown in Figure 1 so as to enable detection of the removal of a portable computer from the office. In this case, the reader may again be a stand-alone device incorporating a display or audible alarm 311 (Figure 3B) which is set off in response to unauthorised removal of a portable computer from the room. Alternatively, as illustrated very diagrammatically by Figures 10 and 11, the reader 300 may communicate via its communications interface 310 with a central control system using any of the known communications protocols used for the existing PARSEC system, for example the communication may be via an RS232, RS485 or WIEGAND communications protocol. Figure 10 shows six readers 300 communicating with such a control system 400. In this example, each of the readers 1 to 6 is provided in a different office or room of the same building.

Generally, as shown schematically in Figure 11, the control system 400 will consist of a control system processor and associated memory 401, a display 402 for

displaying information to a system controller or security officer, a user input device 404 such as, for example, a mouse and/or keyboard for enabling information to be input to the control system processor by a security officer or system controller and possibly also an output device 420 which may be, for example, a printer for providing a hard copy of status reports received by the control system or a communications interface for communicating with other similar control systems.

There are several ways in which both the "home" or "friendly" signal detection system and the "vicinity detection" system may be implemented as set out below.

In a first example, the RF transponder of the card 200 is arranged to continually transmit a short range (low gain) RF signal which can only be detected by the RF transponder of the RF interface 305 of the reader 300 when the card 200 (and thus the portable computer with which the card is associated) is in the immediate vicinity of the exit or door 400 so that it is evident that the portable computer is about to be removed from the office. The distance from the reader 300 at which the portable computer can be detected will be determined by the transmission range of the signal from the card 200

and the reception range of the reader 300, both of which may be adjusted by adjusting the gain of the respective RF transponders. Although this is a relatively simple approach, it does require the card 200 to be transmitting the vicinity signal continually. The card 200 will generally only draw on its internal battery 204 when the portable computer is switched off. However continued transmission of the vicinity signal will increase the load on the portable computer battery unless the portable computer is mains-powered when in the office. In addition because the card is continually transmitting the vicinity signal, the portable computers must be located outside the range of detection of the vicinity signal during their normal use and this may be difficult where the office space is quite small.

Where the RF transponder of the reader 300 is capable of transmitting as well as receiving RF signals, then a number of different options are available. In one example, the RF transponder of the reader may transmit a single RF signal and the card 200 may be adapted to use that signal both as the "home" or "friendly" signal and as a trigger to generate a response RF signal of low gain and thus short range so that the reader 300 can only detect the response signal from the card 200 when the

portable computer carrying the card is in the vicinity of the reader. Again, the range over which the reader 300 can detect the card 200 may be adjusted by adjusting the gains and thus the ranges of the card 200 and the reader 300 transponders. Although this arrangement also requires the reader 300 to have transmission capabilities it has the advantage that the card 200 is not continually transmitting a signal but only responds to a signal received from the reader 300 so reducing the drain on the power supply of the portable computer 100. As a modification of that system, the RF interface 205 of the card 200 may have different gain RF receiver circuits for the "home" or "friendly" and "vicinity" signal detection and its processor 201 may be programmed so as to cause the RF transponder to respond with a transmission only when the low gain "vicinity" signal receiver detects a transmission from the receiver which, because of the low gain of the "vicinity" signal RF receiver of the card 200 will only occur when the card and thus the portable computer carrying the card is in the vicinity of the reader 300. Again, this reduces the drain on the power supply of the portable computer because the card 200 only transmits in response to receipt of the "vicinity" signal. However, again, the area within which the card 200 responds to the vicinity signal is determined by the

gain and thus the reception range of the RF transponder of the card 200. As a further refinement, the processor 301 of the reader 300 may be arranged to cause the RF signal transmissions to be coded so that the "home" or "friendly" and "vicinity" signals are differently coded and the processor 201 of the card 200 may be programmed so as to identify the different codes and only respond by transmission when the "vicinity" signal code is detected. If the "home" or "friendly" and "vicinity" signal are transmitted from the same reader 300, then it will still be necessary for the ranges of the two signals to be different so as to ensure that the card 200 only responds to a "vicinity" signal transmission when it is in the vicinity of the doorway in Figure 1. However, the "home" or "friendly" and "vicinity" signals may have the same range if separate RF transmitters are provided so that, as shown by the dashed box 301 in Figure 1, the "home" or "friendly" RF signal transmission device is located close to the portable computers away from the area covered by the vicinity detection of the reader 300. As another possibility, where it is possible to incorporate a second RF receiver in the card 200, then the "home" or "friendly" signal may be of a different frequency to the "vicinity" signal so that the card 200 only responds by transmission when the "vicinity"

frequency signal receiver of the RF interface 205 detects the "vicinity" signal. Again, however, the arrangement must be such that the vicinity signal can only be detected by the cards 200 when they are in the vicinity of the doorway so that either the "vicinity" signal is of shorter range than the "home" or "friendly" signal or physically separate RF transmitters are provided for the "home" or "friendly" and "vicinity" signals as illustrated by the boxes 300 and 301 (shown in dashed lines in Figure 1) so that the "home" or "friendly" signal transmission device 301 is located physically closer to the portable computers.

Encoding the "home" or "friendly" signal as described above has further advantages as will be described below and accordingly the "home" or "friendly" signal may be encoded in any of the options described above and also where there is no vicinity detection, that is where the only transmission received by the cards 200 is the "home" or "friendly" signal enabling the cards to determine whether they are at their home or base location. The advantage of encoding the "home" or "friendly" signal is that different "home" or "friendly" signal transmitters in different areas (for example in different offices or different parts of a building) may have different codes

and the processor 201 of the card 200 may be programmed so as to identify the location of the portable computer 100 carrying the card from the code of the "home" or "friendly" signal transmission so either allowing or not allowing movement of the portable computer from office to office, depending upon the programming of the processor 201 and the specific code transmitted by the "home" or "friendly" signal transmission devices in different offices or rooms.

In the above-described embodiments, the access control system provided by the cards 200 and the RF signal transmission device is a standalone system, that is, neither the card 200 nor the portable computer 100 with which the card is associated reports its status to any other device, for example a central security control device. However, where the portable computers 100 are coupled to a conventional computer network, then the portable computers 100 may be arranged to report status information received from their associated cards 200 over the network to a central security control device to enable, for example, the system administrator or a security officer to keep a central check on the status of the portable computers.

Where the RF interface 205 of the card 200 includes an RF transmitter as well as an RF receiver, then the processor 201 of the card 200 may be programmed so as to report via an RF transmission information regarding its status to the control system 400 shown in Figure 10 each time it communicates with the control system or periodically or whenever motion, tampering or disconnection is sensed, for example. Where this facility is provided, then the "status" and "vicinity" signal transmissions from the cards will be differently encoded so that the processor 301 of the reader 300 can determine whether the signal being received from a card 100 is a response to a "vicinity" signal transmission from the reader 300 or a "status" signal. The cards 200 may be programmed so as to transmit a status signal to the reader 300 in addition to providing status information to the processor 101 of the portable computer 100 each time the portable computer 100 requests status information. Alternatively, the reader 300 may be arranged to transmit encoded status signal requests so that the cards 200 can respond independently to status signal requests from the reader 300 and from the portable computer 100. In addition, the processor 201 of the card 200 may be arranged to communicate directly with the reader 300 if it detects certain events, for example tampering or disconnection of

the card.

Figure 12 shows a modified form of the flowchart shown in Figure 8 to illustrate the operations carried out by the processor 201 of the card 200 when the card 200 is adapted to communicate with a reader 300 in such a manner. Steps S230 to S235 are the same as in Figure 8 and will not be described again. However, once the processor 201 has reported the results of its status check to the portable computer 100, the processor 201, in this example, determines whether the check on the tamper circuit indicated that tamper had been detected at step S236 and, if the answer at step S236 is yes, controls the RF interface 205 so as to send a tamper signal to the reader 300 at step S237. If the answer at step S236 is no, then the processor 201 determines whether the check on the disconnect sensor at step S232 indicated disconnection had been detected at step S238 and, if so, controls the RF interface 205 so as to send, at step S239, a disconnection signal to the reader 300. As indicated above, it will also be appreciated that steps S236 and S238 could be carried out in reverse order.

When the reader 300 receives any form of status signal from a card 200, it will communicate this to the control

system 400 via the communications interface 310 to cause the control system processor 401 to display to a security officer or system controller a message including the status information. For example, as indicated in Figure 13, when the reader 300 receives a tamper signal at step S300 in Figure 13, the processor 301 will communicate with the control system 400 via the communications interface 310 to cause the control system processor 401 to display to the security officer or system controller a message on the display 402 indicating that it has detected tampering with a card of a portable computer within its range. The signal sent out by the cards 200 may include information identifying the card and/or the associated portable computers. For example, the signal may include the card's identity number so enabling the security officer or system controller to determine exactly which card, and using a database relating cards to portable computers, which portable computer is being tampered with (step S301 in Figure 13). If, at steps 302 in Figure 13, the processor 301 receives via the RF interface 305 a signal from a card 200 indicating that the card has been disconnected and reinserted, then the processor 301 will again communicate via the communications interface 310 with the control system 400 to cause the control system processor 401 to display to

the security officer or system controller a message on display 402 indicating that a card has been removed and replaced. The security officer or system controller may then take appropriate action depending on whether or not the security officer or system controller has information indicating that the removal and reinsertion of the card was authorised. The processor 301 may also cause the alarm 311 to be activated (step S301).

In the above described examples, the presence of a card 200 in the vicinity of a doorway is detected. The system may however also be used to detect the presence of the card in the vicinity of any entrance or exit or the presence of the card in the vicinity of a predefined area which may not have any physically defined entrance or exit. For example, the vicinity detection signal may be used to detect when a portable computer is being taken from or into a defined area. The defined area may be an office, other room, clean room, area of a factory floor or laboratory etc.

Where, as described above, the reader 300 is provided to enable detection of a card 200 and thus a portable computer in the vicinity of an exit or entrance such as a doorway, then the system may be modified to enable

certain personnel, identified by personnel tags or other electronic identification devices similar to the cards 200, to take certain items of equipment into or out of a defined area, for example to remove one of the portable computers 100 shown in Figure 1 from the office through the doorway. Figure 14 shows a flowchart illustrating steps that may be carried out by the reader processor 301 in this circumstances.

Thus, when a person carrying a portable computer 100 comes into the vicinity of the defined area, a "vicinity" RF signal transmitted by the card 200 will be detected by the reader 300. Any of the methods of vicinity detection described above may be used. If the person carrying the portable computer 100 is also wearing a personnel tag from the PARSEC range produced by Newmark Technology, then the reader 300 will also detect a "vicinity" RF signal from that personnel tag. When, as indicated by step S303 in Figure 14, the reader 300 detects the presence of a card 200 and a personnel tag in the vicinity of the prohibited area (the doorway in Figure 1), then, at step S304, the processor 301 checks the received signals for a first identity code identifying a card 200 and a second identity code identifying a personnel security tag. Then, at step 305, the processor

301 checks, if a personnel ID was identified in the return signal, whether the person associated with that ID is authorised to remove a portable computer from this particular room. If the answer at step S305 is that no personnel ID was received or the ID of a person not authorised to remove a portable computer from that room was received, then, at step S306, the processor 301 will communicate with the control system so as to advise the security officer or system controller at step S306 that unauthorised removal of a portable computer from the particular room is being attempted and may also cause the alarm 311 to be activated or other automatic security action to be initiated.

If the processor 301 determines that the person is authorised at step S305 then, at step S307, the processor 301 checks that that particular authorised person is authorised to remove that particular portable computer by checking in a database stored in its memory and associating the personnel IDs with the card IDs of the portable computers, if any, that they are allowed to remove. If the answer at step S307 is that that particular authorised person is not authorised to remove that particular portable computer, then the processor 301 proceeds to step S306. Where the information contained

on the portable computers in a particular room is particularly sensitive, then the reader 300 may be coupled to an electronic door mechanism which, when the reader detects an unauthorised attempt to remove a computer enables the reader 300 to disable the door lock so that exit from the room is not possible in addition to advising the system controller.

The processor 301 may be arranged so as to determine that a particular personnel ID is associated with a particular card ID when the reader receives those two IDs within the same predetermined time window, for example where one ID is received up to 2 seconds before or 2 seconds after the other.

It will be appreciated that, where the reader is part of a security system such as shown in Figure 10, the steps S304 to S307 will generally be carried out by the control system 400 with the reader 300 simply transmitting the received information to the control system.

In the above-described embodiments, it is the cards 200 that communicate with the reader 300. However, communication with the reader 300 may be via the computer 100 and, for example, communication may be via an

infrared or hard wired network rather than an RF link.

In the above-described embodiments, the access control device is provided by a PCMCIA card. However, the access control device may alternatively be provided as a device which is connectable to another interface such as the serial or parallel interface port 106 or 108 of the personal computer. Communication between the signal transmission device or reader 300 and the access control device need not necessarily be by RF but may be by infrared, over a network or the mains electricity supply.

In the above-described embodiments, the items of equipment to be protected are portable computers such as laptops or notebooks or even palm tops. The present invention may, however, also be applied to protect or control access to desktop computers and other items of computer-controlled office equipment, that is office equipment which includes a processor, for example, modern photocopiers, printers and the like. The present invention may also be provided to control access to other types of equipment that include processors such as, for example, video cassette recorders, TVs and the like.

The present invention may also be used to control access

to other items of equipment which, at least in some aspects, are computer or processor-controlled or require computer or processor functions to operate such as computer or processor-controlled machinery in a factory or laboratory. The present invention may be applied to items of equipment such as vehicles and the like fitted with some form of computer or processor control which can accept a card 200 so that, for example, if the card 200 does not receive a "home" or "friendly" transmission within a predetermined time, the vehicle cannot be operated. This may have particular application for expensive items of equipment such as plant hire equipment (forklift trucks, diggers and the like) enabling the items of plant hire equipment to be disabled if they are taken out of a designated area for greater than a predetermined time which may be preset to be, for example, zero if required.

An access control device having the capability to transmit both long and short range transmissions may be used in circumstances where the access control device is not necessarily associated with computer-controlled equipment. For example, the access control device may in such circumstances be a personnel security tag providing relatively long range transmissions to enable a security

system to check that the person wearing that tag is in a specific area and providing relatively short range transmissions to enable a security system to determine when that person leaves or enters a predefined smaller area within the general area.

CLAIMS:

1. A computer, comprising:

a processor;

a memory;

a user-operable input device for enabling a user to control operations of the processor; and

an access control device comprising means for receiving a transmission from outside the computer, wherein access to use of the computer is inhibited unless the access control device receives such a transmission.

2. A computer according to claim 1, wherein the processor is operable to prevent access unless periodic transmissions are received by said access control device.

3. A computer according to claim 1 or 2, wherein the processor is operable to prevent access to use of the computer by a user when a predetermined time has elapsed since the receipt of a transmission by the access control device.

4. A computer according to any one of claims 1 to 3, wherein the receiving means comprises RF signal receiving means.

5. A computer according to any one of the preceding claims, wherein the access control device comprises means for determining whether the access control means has been disconnected and the processor is operable to prevent use of the computer when the access control device determines that it has been disconnected.

6. A computer according to any one of the preceding claims, wherein the access control device comprises means for determining whether the access control means has been tampered with and the processor is operable to prevent access to use of the computer by a user when the access control device determines that it has been tampered with.

7. A computer according to any one of the preceding claims, wherein the processor means is operable to check the access control device during boot-up of the computer.

8. A computer according to claim 7, wherein the processor means is operable to prevent completion of the boot up procedure when the access control device does not report that its status is satisfactory.

9. A computer according to any one of the preceding

claims, wherein the processor means is operable to determine whether the status of an access control device is satisfactory before enabling writing to or reading of data from the memory of the computer.

10. A computer according to any one of the preceding claims, wherein the access control device comprises means for transmitting information to a security control system.

11. A computer according to any one of the preceding claims, wherein the access control device is coupled to an interface of the computer.

12. A computer according to claim 11, wherein the access control device comprises a PCMCIA card and the interface comprises a PCMCIA interface.

13. An access control device connectable to a computer, the access control device comprising: means for receiving a transmission from a device other than the computer and means for communicating with the computer to enable access to use of the computer to be prevented if a transmission is not received.

14. An access control device connectable to a computer, the access control device comprising: means for receiving a transmission from a device other than the computer and means for communicating with the computer to enable access to use of the computer to be prevented when a predetermined time has elapsed since the receipt of a transmission by the access control device.

15. A device according to claim 13 or 14, wherein the receiving means comprises RF signal receiving means.

16. A device according to any one of claims 13 to 15, comprising means for determining information as to whether connection to the computer has been interrupted and means for communicating with the computer to enable access to use of the computer to be prevented when the access control device determines that the connection has been interrupted.

17. A device according to any one of claims 13 to 16, comprising means for determining information as to whether the access control means has been tampered with and means for communicating with the computer to enable access the computer to be prevented when the access

control device determines that it has been tampered with.

18. A device according to any one of claims 13 to 17, comprising means for transmitting information to a security control system.

19. A PCMCIA card comprising a device according to any one of claims 13 to 18.

20. An item of equipment comprising a computer in accordance with any one of claims 1 to 12, a device in accordance with any one of claims 13 to 18 or a PCMCIA card in accordance with claim 19.

21. A security system comprising a plurality of items of equipment in accordance with claim 20 and means for detecting the presence of an item of equipment in the vicinity of a doorway or exit.

22. A control system for monitoring movement of items of equipment, comprising: a database storing information associating each of a plurality of items of equipment with an identified person or each of a number of identified people; means for receiving information

identifying the presence of items of equipment and personnel in the vicinity of a defined area; and processor means operable, when information is received by the receiving means identifying the presence of a person and an item of equipment in the vicinity of the defined area, to determine from the database whether the identified person is associated with that item of equipment in the database and to determine that access to the defined area is unauthorised if the identified person is not associated with the identified item of equipment in the database.

23. A control system according to claim 22, wherein the defined area is a doorway.

24. A control system according to claim 22 or 23, wherein the receiving means is operable to receive information provided by transmissions from identity cards carried by items of equipment and personnel.

25. A control system according to claim 22, 23 or 24, wherein the receiving means is operable to receive information from an identity card reader provided in the vicinity of the designated area.

26. A control system according to claim 22, 23 or 24, wherein the receiving means comprises an identity card reader provided in the vicinity of the designated area.

27. A control system according to claim 26, wherein the card reader is operable to detect radio frequency transmissions from identity cards.

28. A control system according to any one of claims 22 to 27, wherein the processor is operable to cause a warning to be issued if it determines that an identified person is not associated with an identified item of equipment in the database.

29. A control system according to any one of claims 22 to 28 in combination with a computer in accordance with any one of claims 1 to 12 or an access control device in accordance with any one of claims 13 to 18 or a PCMCIA card in accordance with claim 19.

30. A security device adapted to be associated with an item of equipment or a person, the device comprising:

first transmission generating means for generating a first transmission communicating information regarding

the status of at least one of the security device and an item of equipment or person with which the security device is associated and second transmission generating means for generating a second transmission having a shorter range than the first transmission so that the second transmission can only be detected when the security device is in the vicinity of a defined area.

31. A device according to claim 30, wherein the first and second transmission generating means are arranged to generate RF transmissions.

32. A device according to claim 30 or 31, wherein the security device is arranged to couple to an interface of a computer.

33. A device according to claim 32, wherein the device comprises a PCMCIA card.

34. A signal carrying processor implementable instructions for causing a processor to become configured to provide functional components of a computer in accordance with any one of claims 1 to 12, a device in accordance with any one of claims 13 to 18 and 30 to 33,

a PCMCIA card in accordance with claim 19 or a control system in accordance with any one of claims 22 to 29.

35. A storage medium carrying processor implementable instructions for causing a processor to become configured to provide functional components of a computer in accordance with any one of claims 1 to 12, a device in accordance with any one of claims 13 to 18 and 30 to 33, a PCMCIA card in accordance with claim 19 or a control system in accordance with any one of claims 22 to 29.

Application No: GB 0007017.7 54 **Examiner:** Matthew J. Tosh
Claims searched: 1-21 **Date of search:** 7 November 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): G4A (AAP)

Int Cl (Ed.7): G06F 1/00

Other: ONLINE: EPODOC, WPI, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0777171 A1	(C-SAM). See whole document.	1-4 11,13,15 20
X	WO 99/24894 A1	(DATASEC ELECTRONIC GMBH). See abstract.	1-4,11-15 19,20
X	WO 99/11022 A1	(XYDIS). See especially line 17, page 5 to line 6, page 7 and figures.	1-4,7,11 13-15,20
X	WO 98/07249 A1	(CALIFORNIA WIRELESS INC.). See lines 9-23, page 3 and Figs. 1-3.	1,4,11,13 15,20
X	US 5821854	(MOTOROLA). See description.	1-4,11 13-15,20
X	US 5712973	(IBM). Note lines 5-10, col. 7 and line 63, col. 13 to lines 22, col. 14.	1,4,20
A	DE 19843372 A1	(LEGUIN). See WPI abstract and figure.	

X Document indicating lack of novelty or inventive step
Y Document indicating lack of inventive step if combined with one or more other documents of same category.
& Member of the same patent family
A Document indicating technological background and/or state of the art.
P Document published on or after the declared priority date but before the filing date of this invention.
E Patent document published on or after, but with priority date earlier than, the filing date of this application.